EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article ICST.ORG

Adaptations of Personal Health Record Platform for Medical Research on Chronic Diseases

A. Krukowski [1]* and E. Vogiatzaki [2]

[1] Intracom S. A. Telecom Solutions, Peania, Greece
[2] Research for Science, Art and Technology (RFSAT) Ltd, Sheffield, United Kingdom

Abstract

The article reports on experiences in e-Health platforms and services for supporting medical research into the causes and relationships among physiological parameters and health problems concerning different chronic diseases. The Personal Health Record (PHR) is a way of standardizing electronic management of medical information between patients and their physicians, including medical bodies collaborating in providing integrated medical care services. We describe roles and aims behind electronic health records, follow with applicable legal and standardizations frameworks and relevant European activities, leading to the presentation of common commercial and open-source implementations of such systems, concluding with the indication of specific adaptations enabling a use of stored personal health data for scientific research into causes and evaluation of chronic illnesses. We describe ethical and privacy concerns that are relevant to using and exchanging electronic health information.

Keywords: Personal Health Records; Chronic Diseases; Anonymity, Privacy.

Received on 09 October 2014, accepted on 27 February 2015, published on 18 May 2015

Copyright © 2015 A. Krukowski and E. Vogiatzaki, licensed to ICST. This is an open access article distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/phat.1.1.e5

*Corresponding author. Email: krukowa@intracom-telecom.com

1. Introduction and motivation

Epilepsy, the propensity for recurrent, unprovoked epileptic seizures, is the most common serious neurological disorder, affecting over 50 million people worldwide. Epileptic seizures manifest with a wide variety of motor, cognitive, affective, and autonomic symptoms and signs and associated changes in the electrical activities of the brain electroencephalography (EEG), the heart electrocardiography (ECG), muscle electromyography (EMG), galvanic skin response (GSR), as well as changes in other important measurable biological parameters, such as respiration and blood pressure.

Their recognition and full understanding is the basis for their optimal management and treatment, but presently is unsatisfactory in many respects. Epileptic seizures occur unpredictably and typically outside hospital and are often misdiagnosed as other episodic disturbances such as syncope, psychogenic and sleep disorders, with which they may co-exist, blurring the clarity of information presented to clinicians; on the other hand, costs of hospital evaluation are substantial, frequently without the desirable results, due to suboptimal monitoring capabilities.

Reliable diagnosis requires state of the art monitoring and communication technologies providing real-time, accurate and continuous multi-parametric physiological measurements of the brain and the body, suited to the patient's medical condition and normal environment and facing issues of patient and data security, integrity and privacy. The purpose of the FP7 projects “Advanced multi-parametric monitoring and analysis for diagnosis and optimal management of epilepsy and related brain disorders” (ARMOR) and StrokeBack is to manage and analyse large number of already acquired and new multimodal and advanced medical data from brain and

body activities of epileptic patients and controls (MEG, multichannel EEG, video, ECG, GSR, EMG, etc.) aiming to design a holistic, personalized, medically efficient and affordable system for detecting abnormal condition and aid in efficient rehabilitation.

New methods and tools have been already developed for multimodal data pre-processing and fusion of information from various sources [1-3]. Novel approaches for large scale analysis (both real-time and offline) of multi-parametric streaming and archived data have been developed able to discover patterns and associations between external indicators and mental states, detect correlations among parallel observations, and identify vital signs changing significantly. Methods for automatically summarizing results and efficiently managing medical data are also being developed. The project incorporates models derived from data analysis based on already existing communication platform solutions emphasising on security and ethical issues and performing required adaptations to meet specifications.

ARMOR aims to provide flexible monitoring optimized for each patient and will be tested in several case studies and evaluated as a wide use ambulatory monitoring tool for seizures efficient diagnosis and management including possibilities for detecting premonitory signs and feedback to the patient. Therefore, our goal is to develop a personalized system that assists in diagnosis, prognosis and treatment of the disease. Such system should fulfil the following criteria; it should be non-invasive, mobile, continuous and unobtrusive, whereas all possible security and privacy aspects should be taken into account. Since access to large amounts of medical data is required for deriving all necessary models, a special effort is devoted to ensuring data anonymity, protection and restriction of access to private information in the whole system.

2. Personal Health Record (PHR) System

The core system dealing with patient medical data in e Health related services and applications, like ARMOR, is the Electronic Health Record (EHR), defined as digitally stored health care information about individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times. A patient's healthcare information may be spread out over a number of different institutes that do not interoperate. In order to provide continuity of care, clinicians should be able to capture the complete clinical history of the patient.

The Personal Health Record (PHR) is the electronic part of the health-related in-formation of a person (such as diagnoses, medications, allergies, lab test results, immunization records but also administrative tasks such as appointment or prescription renewals) that can be extracted from multiple sources, but always under the control of the consumer, patient or informal caregiver. This is the most important difference between the PHR and the EHR or electronic medical record, which is maintained by the healthcare providers and payers.

The EHR standardisation [4] aims to ensure that patient records are used to support shared care among clinicians with different specialisations, while enabling the mobility within and among countries for people who give and receive healthcare. Since EHR systems store sensitive patient data, ethical and privacy regulations apply [5].

3. Ethical Regulations and Directives for Privacy and Managing Medical Data

One of the most controversial issues for PHRs is how the technology could threaten the privacy of patient information. Network computer break-ins are becoming more common, thus storing medical information online can cause fear of the exposure of health information to unauthorized individuals. In addition to height, weight, blood pressure and other quantitative information about a patient's physical body, medical records can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders, and diseases, etc. Various threats exist to patient information confidentiality, example of are:

- *Accidental disclosure*: during multiple electronic transfers of data to various entities, medical personnel can make innocent mistakes to cause its disclosure.
- *Internal leaks*: medical personnel may misuse their access to patient information out of curiosity, or leak out personal medical information for profit, revenge, or other purposes.
- *Uncontrolled secondary usage*: those who are granted access to patient in-formation solely for the purpose of supporting primary care can exploit that permission for reasons not listed in the contract, such as research.
- *External intrusion*: Former employees, network intruders, hackers, or others may access information, damage systems or disrupt operations

Unlike paper-based records that require manual control, digital health records are secured by technological tools. Rindfleisch [6] identifies three general classes of technological interventions that can improve security:

- *Deterrents* – These depend on the ethical behaviour of people and include controls such as alerts, reminders and education of users. Useful form of deterrents is Audit Trails, recording identity, times and circumstances of users accessing information. Users aware of such a record keeping system, are discouraged from taking ethically inappropriate actions
- *Technological obstacles* – These directly control the ability of a user to access in-formation and ensure that users only access information they need to know ac-

cording to their job requirements. Examples of technological obstacles include authorization, authentication, encryption, firewalls and more.

- *System management precautions* – This involves proactively examining the in-formation system to ensure that known sources of vulnerability are eliminated. An example of this would be installing antivirus software in the system

The extent of information security concerns surrounding PHRs extends beyond technological issues. Each transfer of information in treatment process must be authorized by patients even if it is for their benefit. No clearly defined architectural requirements and information use policies are yet available. While the trends and developments of ICT in healthcare have given rise to many positive developments, concerns about the use of ICT in user services mainly concentrate on the difficulty of respecting privacy and confidentiality when third parties may have a strong interest in getting access to personal health data electronically recorded and stored and difficulty in ensuring the security of shared personal data [7].

Therefore the project is dedicated to respecting and protecting the personal data, considered as extremely sensitive since they refer to the identity and private life of the individual. It recognises the intent to create a potential for the circulation of personal data, across local, national and professional borders, giving such data an enhanced European dimension, while respecting the principles of the European Convention of Human Rights, the rules of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and especially the European Directive 95/46/EC, for the protection of personal data will be strictly followed when addressing ethical issues.

A. Involving adult healthy volunteers

Potential ethical issues that are addressed in this research will involve end user interviews, questionnaires and trialling of prototype systems during the development and testing. The right to privacy and data protection is a fundamental right and therefore volunteers have the right to remain anonymous and all research will comply with Data Protection legislation regarding ICT research data related to volunteers.

During the research in ARMOR only participant who has sufficient cognitive and physical ability to be able to safely participate and clearly give informed consent are asked to participate. Potential ethical issues arise from the fact that participants, especially those who may tire easily or become distressed. Ethical issues may also arise when the system is used to give participant location or wellbeing information to third parties. Here release of this information is subject to informed consent of participants, and subject to the ethical frameworks to restrict knowledge of this information to only those given consent.

All participants in the research are volunteers enrolled from the end user groups connected with this research and all ethical criteria are supervised by ethicists. At all times participants are ensured privacy and technical platform managing private user data is fully geared to enforce ethics.

B. Tracking the location of people

Tracking the location of people is tightly linked with services delivered at the location of the user. This requires new look at the new socio-legal issues they raise. In the ARMOR project we only consider laws applicable to protecting privacy of the general population and NOT the laws and regulation specific for the case of the employee tracking and localization.

The European legislation has adopted specific rules requiring that the consent of users or subscribers be obtained before location data are processed, and that the users or subscribers be informed about the terms of such processing. The rule is that the applicable law is that of the Member State where the "controller" is established; and not that of the Member State of which the data subject is a national. "If the controller is not established in a Member State, and in that case data protection laws of the 3rd country should be found adequate by the EU-Commission." [8]

Location data collection will be in accordance with some basic principles: finality, transparency, legitimacy, accuracy, proportionality, security and awareness. Access to location data must be restricted to persons who in the course of exercising their duties may legitimately consult them in light of their purpose. The relevant laws include:

- *Directive 95/46/EC*: Protection of individuals with regard to processing of personal data and free movement of such data [9]
- *Directive 2002/58/EC*: Processing of personal data and protection of privacy in electronic communications [8]
- *Directive 58/2002/EC* of the European Parliament and of the Council of 12th July 2002 [10]

Processing of personal data and the protection of privacy in electronic telecommunications sector is governed by:

- *Directive 97/66/EC*: Data Protection in the Telecommunications Sector [11]
- *Directive 99/5/EC*: Radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [12]
- *Art. 29 - Data Protection Working Party*: Working Document on Privacy on the Internet

C. Specific approaches adopted

The consent of users or subscribers shall be obtained before location data needed for supplying a value-added service are processed. Users or subscribers will be informed about the terms of such use. Access to location data must be restricted to persons who in the course of exercising their duties may legitimately consult them in the light of their purpose. All required user profile data are stored upon his/her mobile device and be securely protected.

Relevant preferences relate to his/her diet, physical activities, dietary or transport/tourism related preferences, and, in general, simple everyday task preferences will not be stored locally. The user will have the capacity to view/hear, change or delete, as he/she wishes, all stored data by the system (including his/her profile data), with the help of a very simple and multimodal interaction (touch, buttons and voice input supported).

Types of data to be retained under categories identified in Article 4 of Directive 95/58 of 12th July, 2002. Specific safeguards - issues considered by the Article 29 working parties to be addressed with regard to the retention of data processed in connection with the provision of public electronic communication services (21st October 2005 opinion on the same subject directive proposal issued by the EU Commission on 21st September 2005).

4. Authentication and Authorisation

Authentication and authorisation are two main means for allowing access for the user to a resource. Authentication involves such issues like identifying the user by means of either a simple login / password check to elaborate biometric analysis involving fingerprints, retina scans, and voice and /or face recognition etc. Authorisation then performs checks whether a given user may be granted access to a given resource or not.

Such processes have been part of any secure system from the beginning of computing systems. Their complication has increased recently with the rapid growth of the amount of information resources and number of user accounts in each system, platform and/or network. This increases network administrators' work on properly securing their network and databases against un-authorised access at the same time providing users' with uninterrupted access to resources that they should be authorised to access.

However, currently employed methods for performing authentication and authorisation, in most cases, require user authentication every time he moves between resources stored on differently protected sites causing annoyance and loss of time. On the other hand approach to authorising users based on user-resource association requires tedious administrators' job to properly secure access to different resources and gives rise to frequent faults when users are either authorised to access resources that they should not have access to or not being able to access those that they should be able to.

This problem has been identified and addressed in almost all the systems since long time [6]. Administrators are offered means for specifying access rights per user group, policy definition mechanisms and macros allowing them to simplify management of access right to both existing and new users. Despite the fact that these tools are used the problems of authentication and authorisation still contain loop holes attributed mostly to human errors than to machine security as such. Our proposed seamless authentication and authorisation is aimed to simplify further the process of securing access to multiple-interconnected systems as well as making authorisation less prompt to faults.

Authentication is the process of authenticating a user across multiple account protected resources and platforms, i.e. agreeing between different authentication authorities means of establishing trust relationships and dependability for transferring users authentication status i.e. checking that a user is who they claim to be. The process will include customisation of means of authentication whereby users will not be required to perform authentication while transferring from one trusted party to another using single authentication.

In the case of moving from a party with lower authentication requirements to one requiring higher level of authentication, user will only be required to perform extra security checks while accessing differently protected resources instead of performing the whole authentication process from the beginning. Approaches like this have been already proposed, most known being Windows Passport or Live Account [13] where user may move between sites that support this technology. However, such methods do not take into account differences between authentication means required by different sites. This limits applicability of technologies to social WEB sites aiming to keep a record of users accessing their services.

Authorisation in computer terms refers to granting access to a resource to a given user. In most computer systems granting access is related to belonging to a specific user group meant to allowing administrators defining single access rights rules for a group of users. However, this makes it very difficult when it comes to more per-user access granting, especially in systems with large number of user accounts. What we propose is to unify and simplify means of granting user access to given resources.

The process will define sets of resource authorisation dependencies whereby access to one resource may be implicitly granted upon prior-assigned access rights to another resource. This will allow removing the need for the security administrator to provide access rights to every user to every resource, instead concentrating on defining security interdependencies between resources and defining user access right only to key global resources. Note, that this will not remove a possibility to explicitly

grant or block access to a given resource to a given user, if required.

5. PHR Platform Implementation

The PHR platform developed internally by Intracom S. A. Telecom Solutions, name intLIFE, has been enhanced and geared to diverse health application through a number of FP7 funded research projects, such as ICT-PSP-NEXES, AAL-PAMAP, FP7-StrokeBack, FP7-ARMOR etc. [14]. Special adaptations made in ARMOR and StrokeBack have been geared to allow safe sharing of patients' clinical data with appropriate measures, as described earlier, for the protection of private data, ensuring controlled access to it while ensuring that any data distributed cannot be traced back to the person from whom data has been taken from. This way the intLIFE system could be safely applied in ARMOR for the purpose of deriving clinical models build from large amount of data for subsequently allowing more reliable feature based clinical diagnosis on other patients and detection of conditions not possible earlier. In order to provide necessary privacy and security safeguards EHR/PHR, Vital Signs Monitoring and Management subsystems are all connected via secure and encrypted interfaces controlled via authentication, authorisation and anonymizing modules.

6. Summary and Feedback

The introduction of EHR/PHR systems is the response to the inherent problem of the medical community in dealing with growing amount of papers and printed type of medical records. This becomes also a matter of costs as much time and money is wasted on copying, faxing, and retrieving paper files. Move to electronically stored and managed patient records is both a simplification of the past problems, while adding new ones.

Hence, governments demand increasingly secure and standard-compliant health records [15]. In today's world, it takes more than a simple document to meet national record keeping guidelines. Electronic Health Records are an obvious solution to all emerging problems in the medical care, offering simplification of growing patient records, stimulates easier exchange of data among medical professionals, contributes to cutting costs of medical care as a whole. Records are accessible by multiple health providers. Subject to providing sufficient safeguards at every level, a complete security of data may be achieved. Through data encryption, password protection, the electronic health record offers a peace of mind that data is kept away from unauthorised eyes. Nevertheless, although the future of e-Health has never looked so bright, there are still several concerns that needs careful attention.

Growth of e-health systems inherently implies that any patient's data may be stored not in one place, but on several diverse systems implying increased risk of leaking information to unauthorised third parties. Cyber security procedures are also not consistent across various systems, implying that some may be easier to break into and increasing vulnerability of data stored there.

What adds to the problem is lack of seamless interoperability among e-health systems based on electronic records. Since early stages of development of HL7 standard [16], now one of the base reference standards for e-health, it was considered only as a set of guidelines and not a factual standard to follow. This has resulted in systems being built and deployed that had implemented only a part of the HL7 specification [17] suited to particular needs of a given service provider. Interoperability among such restricted systems is a tiresome process, resulting in exchanging in-complete information. This deficiency has been recently recognised as critical for future e-health and the HL7 is being evolved to define the base set of interoperability criteria for ensuring smooth collaboration among different health systems. However, this process is still ongoing and requires much more research work, including interoperability at the device level and especially for mobile physiological monitoring.

In conclusion we can observe a dramatic changes in the e-health do-main with the introduction of electronic health records, boosting the efficiency of medical services at a lower cost, at the same time offering still a vast range of re-search challenges that we may expect to be pursued and hopefully resolved in the near future.

Acknowledgements

The research leading to these results has received funding from the European Union Seventh Framework Program (FP7/2007-2013) under grant agreements n° 287720 ARMOR and n° 288692-StrokeBack.

References

[1] Artemis CHIRON project: http://www.chiron-project.eu

[2] FP7 ARMOR Project: http://armor.tesyd.teimes.gr

[3] AAL PAMAP Proejct: http://www.pamap.org

[4] Heubusch, Kevin. IT Standards for PHRs: Are PHRs Ready for Standards? Are Standards Ready for PHRs? AHIMA journal, 2008, vol. 79, no 6: 31-36

[5] ISO/TC 215 Technical Report: Electronic Health Record Definition, Scope and Context, 2nd Draft, August 2003

[6] Rindfleisch T.C. "Privacy, information technology and health care", Communications of ACM, vol 40 issue 8, Aug. 1997, pages 92-100

[7] Eichelberg, M., Aden, T., Riesmeier, J., Dogac, A., Laleci, G., "A Survey and Analysis of Electronic Healthcare Record Standards", ACM Computing Surveys, Vol. 37, No. 4, December 2005, pp. 277- 315

[8] Directive 2002/58/EC:: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058

[9] Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[10] Directive 58/2002/EC: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=OJ:L:2002:010:TOC

[11] Directive 97/66/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31997L0066

[12] Directive 99/5/EC: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31999L0005

[13] MS Live: http://www.microsoft.com/en-us/account/default.aspx

[14] "Next-generation remote healthcare: A practical system design perspective", edited by K. Maharatna and S. Bonfiglio, Chapter 6 by Artur Krukowski, Emmanouela Vogiatzaki et al, "Patient Health Record (PHR) system", Springer Science and Business Media New York, SBN 978-1-4614-8842-2, November 2013 \

[15] HL7 EHR System Functional Model: A Major Development towards Consensus on Electronic Health Record System Functionality, White Paper, 2004

[16] HL7. Health Level Seven International. [Online] 2007. www.hl7.org

[17] SNOMED-CT. SNOMED-CT. [Online] International Health Terminology Standards Development Organisation, 2009, http://www.ihtsdo.org/snomed-ct